Environmental Management Consolidated Business Center (EMCBC)

Subject: Chiquita Center Facility Security Plan

PLAN APPROVED: **(Signature on File)**
EMCBC Director
ISSUED BY: OFFICE OF LOGISTICS MANAGEMENT

1.0 PURPOSE

The purpose of this document is to describe the security activities and posture for the Environmental Management Consolidated Business Center's Chiquita Center facility.

2.0 SCOPE

This Plan addresses security activities and protections pertinent to the EMCBC Chiquita Center facility. It identifies individual employee reporting responsibilities pertinent to all EMCBC employees and support service contractor personnel regardless of where they are assigned.

3.0 APPLICABILITY

This document applies to all DOE employees and support services contractor personnel working at the EMCBC Chiquita Center facility.

4.0 REQUIREMENTS and REFERENCES

4.1 Requirements:

4.1.1 DOE N 206.4, Personal Identity Verification
4.1.2 DOE O 142.3, Unclassified Foreign Visits and Assignments
4.1.3 DOE O 205.1A, Department of Energy Cyber Security Management Program
4.1.4 DOE F 5631.9, Security Termination Statement
4.1.5 DOE M 470.4-5, V.3, Personnel Security
4.1.6 DOE M 470.4-1, Safeguards and Security Program Planning and Management, Part 2, Section N- Tables and Figures.

4.2. Reference:

4.2.1 IP-470-01, Personnel Security, Chapter V, 3.

5.0 DEFINITIONS

Export Controlled Information - Certain unclassified Government information under the Department's cognizance that, if generated by the private sector, would require a specific license or authorization for export under regulations. Information and technology regulated

by the Export Administration Regulations, 15 CFR Parts 742, 744, and 746, and the International Traffic in Arms Regulations, 22 CFR 120.21.

Foreign National - Any person who is not a U.S. citizen; any corporation not incorporated in the U.S.; any international organization; foreign government; or any agency or subdivision of foreign government (e.g., diplomatic missions).

Non-Possessing Facility - A facility which has employees authorized access to classified information or matter, or Special Nuclear Material (SNM) maintained at other facilities. Non-possessing facilities themselves do not possess any classified information or matter, or SNM.

Official Use Only (OUO) - Certain unclassified information that may be exempt from public release under the Freedom of Information Act and has the potential to damage governmental, commercial or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities.

Security Incident - Actions, inactions, or events that have occurred that: 1) pose threats to national security interests and/or Departmental property; 2) create potentially serious or dangerous security situations; 3) potentially endanger the health and safety of the workforce or public (excluding safety related items); 4) degrade the effectiveness of the Safeguards and Security (S&S) program, or 5) adversely impact the ability of organizations to protect S&S interests.

Unclassified Controlled Nuclear Information (UCNI) - Certain unclassified Government information concerning nuclear material, weapons, and components whose dissemination is controlled under 42 U.S.C. 2168 (Section 148, as amended, of the Atomic Energy Act of 1954), DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information, and DOE M 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information.

Visitor - Anyone who is not employed by the EMCBC and who does not possess a DOE standard security badge.

6.0 RESPONSIBILITIES

6.1 EMCBC Director

6.1.1 Approval Authority for the EMCBC Chiquita Center Facility Security Plan

6.2 EMCBC Facility Security Officer

6.2.1 Initiates annual review and revision process for the Chiquita Center Facility Security Plan

6.2.2 Serves as a role holder in the EMCBC's implementation of the HSPD-12 credentialing process

6.2.3 Coordinates the EMCBC's Foreign Visits and Assignments Program, including data entry of visit/assignment requests in the DOE's Foreign Access Central Tracking System (FACTS)

6.2.4 Accepts and processes information reported by employees in conformance with section 8.8 of this Plan

6.2.5 Coordinates the Security Awareness Program for the Chiquita Center Facility

6.3 EMCBC Facility Manager

6.3.1 Maintains spare office keys and 2 facility master keys.

6.3.2 Coordinates EMCBC cleaning, maintenance, and other tenant issues with the Chiquita Center building management staff and General Services Administration personnel.

6.4 EMCBC Assistant Director for Information Management

6.4.1 Manages the EMCBC Unclassified Cyber Security Program

6.5 EMCBC Human Resources Administrative Assistant

6.5.1 Maintains the facility's visitor register and issues/collects visitor security badges at the 5th floor receptionist desk.

6.6 EMCBC Staff

6.6.1 Comply with the Chiquita Center Facility Security Plan by adhering to: security awareness, badging, and visitor protocols; reporting requirements; and other protection measures addressed in this Plan

7.0 GENERAL INFORMATION

The EMCBC was created as an element of the U.S. Department of Energy's Office of Environmental Management (EM) to provide various administrative services to selected EM closure and small sites. Major components of the EMCBC are:

Information Resource Management
Civil Rights and Diversity
Cost Estimating and Analysis Center
Financial Management
Human Resources
Contracting
Legal Services
Logistics Management

Technical Services (provided by a Cadre of personnel trained/experienced in a variety of technical disciplines)

The EMCBC is located on the 5th, 6th, and 7th floors of the Chiquita Center, a commercial office building, located at 250 East Fifth Street, Cincinnati, OH 45202. The office space is leased by the U.S. General Services Administration (GSA) on the DOE's behalf.

The security interests at the EMCBC's Chiquita Center facility consist of sensitive unclassified information and government property.

8.0 PLAN

8.1 SAFEGUARDS AND SECURITY (S&S) PROGRAM PLANNING

The objective of EMCBC management is to establish and maintain a viable, cost-effective, and responsive security program capable of protecting the DOE assets with which it has been entrusted. Activities performed by EMCBC personnel at the Chiquita Center are unclassified. However, classified interests are performed at some of the sites serviced by the EMCBC. Additionally, the EMCBC staffs a facility that serves as the repository for legacy classified records accumulated from DOE closure sites. This facility, commonly referred to as Building 55, is located in the Denver Federal Center. Building 55 has its own Facility Security Plan, and therefore is not addressed in this document.

Although no classified activities are performed at the EMCBC in Cincinnati, some EMCBC personnel assigned to the Cincinnati location are involved with the classified interests at Building 55 and other serviced DOE sites. As an example, the EMCBC is responsible for administration of a cadre of technical experts who are assigned to various DOE locations based upon skills/needs considerations.

The EMCBC facility at the Chiquita Center, Cincinnati, OH is registered as a Non-Possessing facility, reflecting the maintenance of some personnel security clearances and the absence of classified activities/matter at this location. The EMCBC has been assigned facility code 12531. Work at the EMCBC includes performance of a number of activities, primarily in the contracts, legal, and personnel functional areas, involving sensitive unclassified information. S&S planning efforts are largely focused on developing practices aimed at protecting this sensitive information, as well as the EMCBC's property and personnel. This Plan identifies the security practices that have been developed and implemented at the EMCBC. The Plan will be reviewed at least annually and updated as required subsequent to that review, or whenever significant changes in the operating environment, including security interests, warrant.

8.2 ACCESS CONTROL AND SECURITY BADGING

8.2.1 Employee Access

Routine employee access to the EMCBC is through one of 2 sets of double doors on either the 5th or 6th floors or through the single set of double doors on the 7th

floor or the single hallway door on the 7th floor. All 4 sets of entry doors are magnetically locked and controlled by a KeriSystems proximity badge reader system. Each employee is issued a proximity card that allows access through all 4 sets of double doors as well as through the stairwell doors on the 5 and 6th floors. Each set of double entry doors includes a Stanley powered handicap accessible door. After the doors have been unlocked by presentation of a proximity card, pushing the handicapped button will cause the door to automatically open. It is the responsibility of persons entering/exiting or otherwise opening the doors to ensure that unauthorized persons do not enter while the doors are unlocked.

Other perimeter doors include: 5th floor east and west stairwells (1 door each); 5th floor door from freight elevator vestibule; 6th floor east and west stairwells (1 door each), and; 6th floor door from freight elevator vestibule.

Proximity card badge readers are also employed internally on both the 5th, 6th and 7th floors. Internally controlled areas include the following:

5th floor – Rm. 549 (Shared File Room – 2 readers), and Rm. 592 (Information Management Work Space – 1 reader)

6th floor – Rm. 652 (Logistics File Room – 2 readers), Rm. 649 (Contracts File Room – 2 readers), 3 hallway doors to Contract's Suite – 1 reader for each of the 3 hallway doors, and Rm. 690 – 1 reader

7th floor – Rm. 710 (Server Room) – 1 reader

The KeriSystems access control system utilizes the Doors Access Control System Software which is operated on a dedicated desktop personal computer. The personal computer is located in Rm. 690, an office to which access is strictly controlled. Access to the software application requires entry of a user name and password. Enrollment in the access control system is performed by employees of the EMCBC's Office of Logistics Management. Proximity cards, along with security badges are obtained from departing employees, and the access afforded by the proximity cards is terminated when they are turned in by departing personnel or reported lost. The software provides a list of enrolled cards and a history of when and to whom they are assigned.

8.2.2 Employee Badging

The EMCBC complies with the requirements of Homeland Security Presidential Directive (HSPD) – 12 and with the DOE's implementing directive DOE N 206.4, Personal Identity Verification (PIV) by ensuring that the identity and eligibility of all persons needing a PIV badge are established. Applicant identity is verified by review of two acceptable forms of identification provided by the applicant. Eligibility is confirmed by verification that applicant has undergone a favorably adjudicated National Agency Check with Inquiries (NACI) or more extensive investigation. The EMCBC intends to issue the HSPD-12 PIV II badge to its

employees by the end of CY2008. At that time the DOE standard badge, which was adopted as the PIV I badge, will no longer be used at the EMCBC.

A local site specific picture badge will be issued to uncleared contractor personnel who have not been opted into the population of personnel covered by the HSPS-12 protocol.

Personnel issued a badge by the EMCBC are expected to wear their badge at all times while in the EMCBC, and to remove or otherwise conceal their badge when they leave the work space.

8.2.3 Visitor Access

A visitor is defined as anyone who does not possess an EMCBC issued badge or who does not possess a PIV I (DOE standard badge with blue, yellow or gray background color) or PIV II style badge. Visitors are required to report to the 5th floor, where they must contact an EMCBC employee to gain physical access. Typically this is accomplished by pressing the door bell located in the passenger elevator vestibule beside the 5th floor north lobby doors. An Administrative Assistant is typically sitting at the receptionist work area just inside the doors. The individual manning the receptionist desk can allow a visitor in without leaving the desk by pushing a door release button which deactivates the magnetic door lock. Once inside, a visitor completes the visitor log and receives a visitor badge.

A visitor must be hosted by an EMCBC employee. It is the responsibility of the EMCBC host to ensure that the visitor does not gain access to work areas or materials unrelated to the visit. The host must also ensure that upon completion of the visit, the visitor is appropriately signed out of the visitor log and the visitor badge is returned to the visitor receptionist area.

Any EMCBC employee is permitted to allow a visitor entry provided the visitor log is completed, a visitor badge is issued, and the visitor is a U.S. citizen.

8.2.4 Foreign National Visits

Foreign national visitors/assignees are approved for access in accordance with the DOE's Unclassified Foreign Visits and Assignments Program and its implementing directive, DOE O 142.3, (Req. 4.1.2). Foreign national visits and assignments require approval by the EMCBC Director.

Visits or assignments involving foreign nationals associated with terrorist countries should be submitted to the EMCBC Facility Security Officer (FSO) at least 2 months prior to the desired start date, while visits/assignments involving sensitive subjects or persons associated with sensitive countries, other than terrorist states, should be submitted at least 4 weeks in advance. Non-sensitive visits and assignments may be submitted 2 weeks prior to the desired start date.

Foreign national visitors are to be escorted at all times.

8.2.5 Locks and Keys

Entry doors from the public elevators are secured with magnetic locks controlled by a KeriSystems Entry Control System. Interior office doors are lockable, and personnel assigned offices are issued a key to their office by the EMCBC Facility Manager or EMCBC security personnel. A database is used to track key issuance and status. A spare key to each office is maintained by the Facility Manager (FM), or by the Assistant Director with cognizance over a particular set of offices. The FM maintains 2 office master keys. Four additional master keys are assigned to other EMCBC staff members. The Chiquita Center's building management company, Grubb & Ellis, has office master keys which they provide to maintenance personnel, building security staff, and cleaning staff personnel as needed. Proximity cards, affording access to the EMCBC, have been provided to designated employees of Grubb & Ellis, and Grubb & Ellis's contracted building security and cleaning staffs. Grubb & Ellis employees and its contracted employees do not have access to Rooms 511/512 (IM), 690 (Security) and 710 (IRM).

Assigned key holders are expected to report lost or stolen keys to either the FM or to the FSO. A case by case assessment of the situation by the FSO may result in replacement of the key core and issuance of new keys.

8.2.6 Building Maintenance, Cleaning and Security Services

Grubb & Ellis is responsible for providing maintenance, cleaning, and security services. The security services provided to the EMCBC are the same services provided to all other Chiquita Center tenants; i.e. a security desk located in the lobby manned 24/7, a service elevator manned by security personnel during regular hours and for special projects, and regular security patrols on the floor after business hours. The building's routine business hours are 6 a.m. to 6 p.m., Monday through Friday. Outside of those hours persons entering the building must show an acceptable form of identification and sign an after hours log. Authorized persons are provided with a specific numerical code necessary to take the pedestrian elevator to the particular floor associated with that code.

Individual offices are vacuumed and have their trash collected nightly by the building's contracted cleaning staff. Cleaning personnel use EMCBC issued proximity cards to enter the EMCBC, and master keys to unlock individual offices. Office doors are closed and locked after the offices are cleaned. Since maintenance, cleaning, and security service personnel have access to individual offices & storage rooms, it is incumbent to secure all sensitive material after hours.

8.3 COMPUTERS AND AUTOMATED INFORMATION PROCESSING

Unclassified information systems, including desktops, laptops, and fax machines, must comply with DOE O 205.1, Department of Energy Cyber Security Management Program, (Req. 4.1.3). All personnel assigned to the EMCBC are provided with computers (either desktops or laptops) connected to the EMCBC's Local Area Network. Individual user accounts on the LAN are password protected. Computers connected to the LAN have a password protected screen saver which activates anytime a computer has been idle for several minutes. Individuals should not share their passwords and must otherwise protect passwords from unauthorized disclosure. The EMCBC's Cyber Security Program Plan provides detailed information regarding mechanisms employed to protect computer and other information processing assets.

8.4 PROTECTION OF SENSITIVE UNCLASSIFIED INFORMATION

8.4.1 General

The EMCBC creates, receives, transmits, uses, reproduces, and destroys sensitive unclassified information. Sensitive unclassified information includes:

Unclassified Controlled Nuclear Information (UCNI)
Official Use Only (OUO)
Export Controlled Information

The identification and subsequent control of sensitive unclassified information will be in compliance with DOE directives and this Plan.

8.4.2 Storage

Sensitive unclassified information must be protected by its holder from unauthorized access.

Given the routine access to EMCBC space by lessor provided cleaning, maintenance, and security personnel, sensitive unclassified information must be locked in a desk or cabinet when the holder is away for the day and at the end of each work day to preclude unauthorized access.

8.4.3 Destruction

Sensitive unclassified documents should be destroyed by authorized cross-cut shredding. The authorized cross-cut shredder is located in the 5th floor mailroom..

8.4.4 Email Transmission

Files containing sensitive unclassified information must be encrypted prior to being transmitted as attachments to email messages addressed to recipients whose email accounts are outside of the EMCBC network. The DOE's encryption application is ENTRUST.

8.5 PERSONNEL SECURITY

8.5.1 Access Authorizations

A number of EMCBC employees hold access authorizations to enable their performance of work activities involving access to classified matter and areas at facilities serviced by the EMCBC. Per a Memorandum of Agreement between the Savannah River Operations Office and the EMCBC, clearance requests for EMCBC personnel are processed by the Savannah River's Personnel Security function. EMCBC management must determine and justify the need for security clearances.

When any cleared employee terminates employment, or otherwise no longer requires a security clearance, a DOE F 5631.9, Security Termination Statement, (Req. 4.1.4), is executed.

8.5.2 Reporting Derogatory Information

Cleared employees must promptly report the types of derogatory or otherwise pertinent information (see 8.8.2) concerning themselves identified in DOE M 470.4-5, V.3, (Req. 4.1.5). (A verbal report must be made within 2 working days followed by written confirmation within the next 3 working days.) This reporting is to be made to the FSO.

8.6 SECURITY INCIDENTS

Security incidents are assigned to one of 4 categories, identified as IMI-1 through IMI-4. These categories and the types of incidents falling under each category are identified in DOE M 470.4-1, Part 2, Section N- Tables and Figures, (Req. 4.1.6).

EMCBC personnel are expected to immediately notify the FSO when unusual or inappropriate security conditions are detected. Such conditions include, but are not limited to: vandalism; theft; malicious destruction of property; threats made against persons or property; unauthorized access; requests for information by unauthorized personnel; unapproved contacts with non-U.S. citizens; and, cyber security episodes, i.e. exploitation attempts, denial of service attacks, etc.

As required, inquiries, to include initial notification and subsequent reporting, will be conducted by a duly appointed inquiry official. If warranted by the circumstances, security infractions will be issued.

Alleged or substantiated criminal violations relating to fraud, waste, and abuse will be reported by the security function to the Office of Inspector General (OIG) and/or the Federal Bureau of Investigation (FBI), as appropriate.

8.7 SECURITY AWARENESS

New employees to the EMCBC are given an initial security briefing whether their position requires them to hold a security clearance (access authorization) or not. This briefing is provided in a read-and-sign format. (Acknowledgement form Attachment B). The briefing document, which is titled "Employee Security Plan" is reviewed annually and updated as needed. Periodic security cautions and reminders are communicated as needed, typically via e-mail messages.

8.8 EMPLOYEE REPORTING REQUIREMENTS

8.8.1 All Employees

A. Report all contacts with persons of any nationality either within the scope or outside the scope of official activities in which; illegal or unauthorized access is sought to classified or otherwise sensitive information, or the employee is concerned that he/she may be the target of exploitation by a foreign entity.

B. Lost or stolen security badges and proximity cards no later than 24 hours after the item is unaccounted for.

C. Incidents of theft, misuse, or malicious destruction of government property.

D. Threats of physical harm associated with the workplace, as well as any actual physical confrontations.

8.8.2 Cleared Employees

A. Report marriage or name change.

B. All arrests, criminal complaints, and detentions, except non-alcohol or drug-related traffic violations resulting in a fine of $250 or less. These matters must be reported within 2 working days of occurrence.

C. Intention to travel to a sensitive country.

D. Change in citizenship.

E. Personal or business-related bankruptcy and garnishment of wages.

F. Employment by, representation of, or other business-related association with a foreign interest or foreign national.

G. Hospitalization for mental illness; treatment for drug abuse; or treatment for alcohol abuse.

8.9 PROHIBITED ARTICLES

In accordance with the General Services Administration Federal Management Regulations that address narcotics and other drugs (102-74.400), alcohol (102-74.405), explosives (102.74-435), and weapons (102-74.440), the following items are, with limited and specific exception, not allowed to be brought into the EMCBC: alcoholic beverages; controlled substances; any weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property.

Legally prescribed and legally possessed narcotics are allowed. Any use of narcotics at the EMCBC must be in conformity with directions provided by the prescribing physician. Weapons carried by federal, state, or local law enforcement personnel may be brought into the EMCBC by such personnel while they are on official business.

9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this Plan are identified as follows:

9.1.1 KeriSystems access control database (proximity card enrollment) – maintained electronically

9.1.2 Individual Personal Identity Verification (PIV) Files

9.1.3 Security Badge Log

9.1.4 Visitor Log, IP-470-01-F2, Access Procedure, (Ref. 4.2.1)

9.1.5 SF-312, Classified Information Nondisclosure Agreement

9.1.6 DOE F 5631.9, Security Termination Statement

9.1.7 Initial Security Orientation Acknowledgement form, PL-470-02-F1

10.0 FORMS USED

10.1 DOE F 206.3, Personal Identity Verification (PIV) Request for DOE Security Badge

10.2 SF-312, Classified Information Nondisclosure Agreement

10.3 DOE F 5631.9, Security Termination Statement

10.4 Initial Security Orientation Acknowledgement form, PL-470-02-F1

11.0 ATTACHMENTS

11.1 Attachment A - Appendix I, EMCBC Chiquita Center Facility Management List
11.2 Attachment B – Initial Security Orientation Acknowledgement form, PL-470-02-F1
11.3 Attachment C - Record of Revision, IP-251-01-F1, Rev. 1

Attachment A

Appendix I

EMCBC CHIQUITA CENTER FACILITY MANAGEMENT LIST

FACILITY MANAGER
Bud Sokolovich — Office: 513-246-0595
EMCBC, DOE — Cell: 513-600-6285

ALTERNATE FACILITY MANAGER
Joanne Merritt — Office: 513-246-0594
EMCBC, DOE — Cell: 513-218-2330

FACILITY SECURITY OFFICER
Patrick L. Vent — Office: 513-246-0605
EMCBC, DOE — Cell: 513-310-4908

EMCBC DIRECTOR
Jack R. Craig — Office: 513-246-0460
EMCBC, DOE — Cell: 513-233-5147

CHIQUITA CENTER MANAGEMENT
Richard D. Purtell — Office: 513-579-1144
General Manager, Grubb & Ellis

Attachment B

INITIAL SECURITY BRIEFING ACKNOWLEDGEMENT

By signing below, I acknowledge having reviewed the EM Consolidated Business Center Initial Security Briefing.

I understand that it is my responsibility to familiarize myself with DOE security requirements as they pertain to my position and work for the Department of Energy, including the review of *PL-470-02, Chiquita Center Facility Security Plan*.

PRINT NAME _____

SIGNATURE _____

DATE _____

Attachment C

EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Original	All	06/11/07
2	Section 4.1 Requirements: **4.1.1** Change to "DOE N 206.4" **4.1.3** Change to "DOE O 205.1A" **4.1.5** Change to "DOE M 470.4-5, Personnel Security, Chapter V, 3." **Section 4.2.1** Change to "IP-470-01, EMCBC Visitor Access Procedure" **Section 6.2.1** Add "Security" following "Chiquita Center Facility" **Section 6.2.2** Change to Serves as a role holder in the EMCBC's implementation of the HSPD-12 credentialing process **Section 7.0** GENERAL INFORMATION To the list of major components of the EMCBC add Cost Estimating and Analysis Center and change "Technical Support" to "Technical Services" Change the sentence beginning "The EMCBC is located on …" to read The EMCBC is located on the 5th, 6th, and 7th floors of the Chiquita Center, a commercial office building, located at 250 East Fifth Street, Cincinnati, OH 45202. **Section 8.2.1** Employee Access change the first sentence to read - Routine employee access to the EMCBC is through one of 2 sets of double doors on either the 5th or 6th floors or through the single set of double doors on the 7th floor or the single hallway door on the 7th floor.	All	07/24/08

Change the sentence that begins "Proximity card badge readers …" to read Proximity card badge readers are also employed internally on the 5th, 6th, and 7th floors.

Add a paragraph 7th floor – Rm. 710 (Server Room) – 1 reader

Section 8.2.5 On last sentence of last paragraph, change "An" to "A" and add "case by case" before assessment of the situation, (and add) "by the FSO" may result in…

Section 8.2.2 – delete existing language and insert the following –

The EMCBC complies with the requirements of Homeland Security Presidential Directive (HSPD) -12 and with the DOE's implementing directive DOE N 206.4, Personal Identity Verification (PIV) by ensuring that the identity and eligibility of all persons needing a PIV badge are established. Applicant identity is verified by review of two acceptable forms of identification provided by the applicant. Eligibility is confirmed by verification that applicant has undergone a favorably adjudicated National Agency Check with Inquiries (NACI) or more extensive investigation. The EMCBC intends to issue the HSPD-12 PIV II badge to its employees by the end of CY2008. At that time the DOE standard badge, which was adopted as the PIV I badge, will no longer be used at the EMCBC.

A local site specific picture badge will be issued to uncleared contractor personnel who have not been opted into the population of personnel covered by the HSPS-12 protocol.

Personnel issued a badge by the EMCBC are expected to wear their badge at all times while in the EMCBC, and to remove or otherwise conceal their badge when they leave the work space.

Section 8.2.3 Visitor Access

Change the first sentence to read – A visitor is defined as anyone who does not possess an EMCBC issued badge or who does not possess a PIV I (DOE standard badge with blue, yellow or gray background color) or PIV II style badge.

Section 8.2.5 Locks and Keys

Change the second sentence to read – Interior office doors are lockable, and personnel assigned offices are issued a key to their office by the EMCBC Facility Manager or EMCBC security personnel. A database is used to track key issuance and status.

Change all references to Triple Net to Grubb & Ellis

Change the last sentence in the first paragraph to read – Grubb & Ellis employees and its contracted employees do not have access to Rooms 511/512 (IRM), 690 (Security), and 710 (IRM).

Section 8.2.6 Maintenance and Cleaning Services – change the name of this section to Building Maintenance, Cleaning, and Security Services.

Section 8.2.6 Add the following sentence at the end of the second paragraph: "Since maintenance, cleaning, and security service personnel have access to individual offices & storage rooms, it is incumbent to secure all sensitive material after hours."

Change the reference to Triple Net to Grubb & Ellis

Section 8.3 Add before the last sentence of the paragraph, "Individuals should not share their passwords and must otherwise protect passwords from unauthorized disclosure."

Section 8.4.1 General – change the first paragraph to read – The EMCBC creates, receives, transmits, uses, reproduces, and destroys sensitive unclassified information. Sensitive unclassified information includes:

Change the last sentence to read – The identification and subsequent control of sensitive unclassified information will be in compliance with DOE directives and this Plan.

Section 8.4.2 Storage

Change the first sentence of the second paragraph to read – Given the routine access to EMCBC space by lessor provided cleaning, maintenance, and security personnel, sensitive unclassified material must be locked in a desk or cabinet when the holder is away for the day and at the end of each work day to preclude unauthorized access.

Section 8.4.3 In the first sentence, where it says "…be destroyed by…" add "authorized cross-cut" shredding. In second sentence, add "authorized" between "the" and "cross-cut". Also add "is" between "shredder" and "located" and add a period after mailroom. Then, omit "is approved for use in this process."

***ADDITION* – 8.4.4** Email Transmission

Files containing sensitive unclassified information must be encrypted prior to being transmitted as attachments to email messages addressed to recipients whose email accounts are outside of the EMCBC network. The DOE's encryption application is ENTRUST.

Attachment C

Appendix I – change the reference to Triple Net Properties to Grubb & Ellis

8.5.2 In the first paragraph, add "(see 8.8.2)" between, "pertinent information" and "concerning themselves."

Appendix I -- Under "Alternate Facility Manager," change "Tim Marcus" to "Joanne Merritt" and update office and cell phone numbers. Also add "Bud Sokolovich's" cell phone number.

2.1	Sections 10 & 11:	10, 11, 12, 14	04/21/09

Numbered the Initial Security Briefing Acknowledge form (already referenced under Records and Forms) and inserted as a new attachment.

CONTROLLED DOCUMENT CHANGE REQUEST

DATE: _____

INITIATOR: _P. Vent_____

INITIATOR PHONE NUMBER: _____

DOCUMENT AFFECTED: _PL-470-02,_____

SECTION: _____ PARAGRAPH #:_____

CONTROLLED NUMBER : _____ PARAGRAPH #:_____

NEW CONTROLLED NUMBER: _____

PROPOSED
REVISION: _Revision and Updating of Plan _____
_____
_____

JUSTIFICATION: __Timely Revision_____
_____
_____
_____

Requested by:
_T. J. Jackson_____ DATE: _____

Approval:
_____ DATE: _____
Associate Director

Assigned to: __P. Vent_____ DUE DATE: _____

IP-251-02-F2, Rev. 1

Document Review Record Sheet				
Document Title	Chiquita Center Facility Security Plan			
IP Number PL-470-02	Revision No. 2	Date Issued for Review 06/17/08		
The subject document is being submitted for your review, approval or comments. Since this review is controlled, a response is required from all reviewers. Therefore, please return the review sheet with or without comments				
To: P. Vent	Extension: 6-0605	By: 06/27/08		
Additional Instructions:				
Reviewer	Approve	Approve w/Comments	Do Not Approve	Signature of Reviewer
B. Fain				
M. Roy				
W. Best				
Acting FM				
B. Everson				
R. Holland				
T. Brennan				
B. Nelson				
T. J. Jackson				
J. Craig				
Comments may be attached to a separate sheet of paper				
APPROVE: Signifies the reviewer's acceptance of the document issued for review.				
APPROVE w/comments: Signifies the reviewer's overall acceptance of the document regarding concept, practice, implementation, provisions and assigned responsibilities. However, the reviewer has suggestions as to the organization of its contents or helpful additions and/or deletions. These comments are termed "non-mandatory comments" and do not require formal resolution between the reviewer and preparer.				
DO NOT APPROVE: Signifies that the reviewer has identified significant problems regarding concept, practice, implementation or responsibilities that render the document unacceptable and/or not in conformance with stated requirements. Such problem areas must be clearly identified by the reviewer. It is mandatory for the preparer to resolve these comments with the reviewer, document the resolution and obtain the reviewers concurrence for the resolution. The reviewer's written concurrence with the resultant change in disposition shall be documented on this form.				
General Review Comments:				
When review is delegated, the designated reviewer shall review and indicate concurrence with the designee's review comments and recommend disposition:				
Designated Reviewer	Concur	Do Not Concur	Signature	Date

IP-251-01-F3, Rev. 1